WHAT IS CLAIMED IS:

1. A data processing device which reads and decrypts encrypted data sets and encrypted key data sets stored in a storage medium, the encrypted data sets being obtained by dividing to-be-stored data into a plurality of divided data sets and then encrypting at least some of the divided data sets for decryption by respectively different key data sets, each of the encrypted key data sets being obtained by encrypting each said key data set for decryption by any one of the other key data sets, the data processing device comprising:

a read-control portion for controlling reading of each said encrypted data set and each said encrypted key data set;

a decryption portion for decrypting the encrypted data set and the encrypted key data set that have been read under the control of the read-control portion; and

a key-data retention portion that retains one of the key data sets that has been decrypted from the encrypted key data set by the decryption portion,

wherein the decryption portion is configured so as to decrypt the encrypted data set and the encrypted key data set based on one of the key data sets that has been already retained in the key-data retention portion.

2. The data processing device of Claim 1, wherein

the read-control portion is configured so as to successively read, in a uniquely determined order, the encrypted data sets and the encrypted key data sets stored in the storage medium, the encrypted data sets being obtained by encrypting all of the divided data sets, the encrypted key data sets being obtained by encrypting the key data sets for decrypting the respective encrypted data sets; and

the decryption portion is configured

so as to decrypt, based on one of the key data sets that is retained in the key-data

retention portion, a first one of the encrypted data sets and a first one of the encrypted key data sets read from the storage medium, and then output a first one of the divided data sets and a first one of the key data sets, and

so as to decrypt, based on the first key data set decrypted and retained in the key-data retention portion, a second one of the encrypted data sets and a second one of the encrypted key data sets read following on the first encrypted data set and the first encrypted key data set.

3. The data processing device of Claim 1, wherein

the read-control portion is configured so as to successively read, in a uniquely determined order,

the encrypted data sets that are said encrypted ones of the plurality of divided data sets stored in the storage medium,

non-encrypted data sets that are the other divided data sets that are stored in the storage medium without being encrypted, and

the encrypted key data sets stored in the storage medium, the encrypted key data sets corresponding to the respective encrypted data sets and the respective non-encrypted data sets; and

the decryption portion is configured in such a manner

that when a first one of the encrypted key data sets and a first one of the encrypted data sets have been read from the storage medium, the decryption portion decrypts the first encrypted key data set and the first encrypted data set based on one of the key data sets that is retained in the key-data retention portion, and then outputs a first one of the divided data sets and a first one of the key data sets,

that when the first encrypted key data set and a first one of the non-

encrypted data sets have been read from the storage medium, on the other hand, the decryption portion decrypts the first encrypted key data set based on another one of the key data sets that is retained in the key-data retention portion, and then outputs the first key data set, and

that the decryption portion decrypts, based on the first key data set, a second one of the encrypted key data sets, or the second encrypted key data set and a second one of the encrypted data sets, read following on the first encrypted key data set and the first encrypted data set, or following on the first encrypted key data set and the first non-encrypted data set.

4. The data processing device of Claim 1, wherein

the read-control portion is configured so as to successively read, in a uniquely determined manner,

the encrypted data sets that are said encrypted ones of the plurality of divided data sets stored in the storage medium,

non-encrypted data sets that are the other divided data sets that are stored in the storage medium without being encrypted, and

the encrypted key data sets stored in the storage medium, the encrypted key data sets corresponding to the respective encrypted data sets; and

the decryption portion is configured in such a manner

that when a first one of the encrypted key data sets and a first one of the encrypted data sets have been read from the storage medium, the decryption portion decrypts the first encrypted key data set and the first encrypted data set based on one of the key data sets that is retained in the key-data retention portion, and then outputs a first one of the divided data sets and a first one of the key data sets, and

that the decryption portion decrypts, based on the first key data set, a second one of the encrypted key data sets and a second one of the encrypted data set sets read after the first encrypted key data set and the first encrypted data set.

5. The data processing device of Claim 1, wherein

the read control portion is configured

so as to read, after reading a first one of the encrypted data sets stored in the storage medium, a second one or any one of second ones of the encrypted data sets which have each been determined beforehand to correspond to the first encrypted data set, and which form a possible-successor group, and

so as to read, in relation to the first encrypted data set, an encrypted-key-data group that includes one or more of the encrypted key data sets which have been obtained by encrypting one or more of the key data sets, the one or more key data sets being used for decrypting the second encrypted data set or sets forming the possible-successor group;

the key-data retention portion retains the one or more key data sets that have been decrypted from the one or more encrypted key data sets forming the encrypted-key-data group that has been read from the storage medium; and

the decryption portion is configured so as to decrypt, based on one key data set that is included among the one or more key data sets retained in the key-data retention portion and that corresponds to the second encrypted data set that has been actually read following on the first encrypted data set, the second encrypted data set and at least one of the encrypted key data sets which has been read in accordance with the second encrypted data set, and which forms an encrypted-key-data group.

6. The data processing device of Claim 1, wherein the data to be stored in the storage

medium includes instructions that the data processing device is made to execute, and branch instructions included among those instructions determine a sequence of reading the encrypted data sets.

7. A data processing device which reads and decrypts encrypted data sets and encrypted key data sets stored in a storage medium, the encrypted data sets being obtained by dividing to-be-stored data into a plurality of divided data sets and then encrypting at least some of the divided data sets for decryption by respectively different key data sets, the encrypted key data sets being obtained by encrypting the key data sets for decryption by a common key data set, the data processing device comprising:

a read-control portion for controlling reading of each said encrypted data set and each said encrypted key data set;

a decryption portion for decrypting the encrypted data set and the encrypted key data set that have been read under the control of the read-control portion; and

a key-data retention portion that retains the common key data set, and one of the key data sets decrypted from the encrypted key data set by the decryption portion,

wherein the decryption portion is configured so as to decrypt the encrypted data set and the encrypted key data set based on one of the key data sets or the common key data set retained in the key-data retention portion.

8. The data processing device of Claim 7, wherein

the key data retention portion includes a first key-data retention portion for retaining the key data set decrypted from the encrypted key data set, and a second key data-retention portion for retaining the common key data set; and

the decryption portion includes a first decryption portion for decrypting the

encrypted data set based on the key data set retained in the first key data retention portion, and a second decryption portion for decrypting the encrypted key data set based on the common key data set retained in the second key data retention portion.

9. The data processing device of Claim 8, further comprising a dummy-read-signal outputting portion that outputs a signal to the storage medium during the period in which the second decryption portion decrypts the encrypted key data set, the signal being the same as a signal for reading a data set stored in an area different from an area in which a data set that will be read next is stored.

10. A data processing method, in which encrypted data sets and encrypted key data sets stored in a storage medium are read and decrypted, the encrypted data sets being obtained by dividing to-be-stored data into a plurality of divided data sets and then encrypting at least some of the divided data sets for decryption by respectively different key data sets, each of the encrypted key data sets being obtained by encrypting each said key data set for decryption by any one of the other key data sets, the data processing method comprising the steps of:

(a) reading one of the encrypted data sets and one of the encrypted key data sets; and

(b) decrypting said one encrypted data set and said one encrypted key data set that have been read in the step (a), and then making a key-data retention portion retain one of the key data sets that has been decrypted from said one encrypted key data set;

wherein in the step (b), said one encrypted data set and said one encrypted key data set are decrypted based on one of the key data sets that has already been retained in the key-data retention portion.

11. A data processing method, in which encrypted data sets and encrypted key data sets stored in a storage medium are read and decrypted, the encrypted data sets being obtained by dividing to-be-stored data into a plurality of divided data sets and then encrypting at least some of the divided data sets for decryption by respectively different key data sets, the encrypted key data sets being obtained by encrypting the key data sets for decryption by a common key data set, the data processing method comprising the steps of:

(a) reading one of the encrypted data sets and one of the encrypted key data sets; and

(b) decrypting said one encrypted data set and said one encrypted key data set that have been read in the step (a), and then making a key-data retention portion retain one of the key data sets that has been decrypted from said one encrypted key data set;

wherein in the step (b), said one encrypted data set and said one encrypted key data set are decrypted based on one of the key data sets or the common key data set that has already been retained in the key-data retention portion.